文章编号:1674 - 2869(2012)10 - 0069 - 04

点对点网络中运用云理论的信任域模型

张　蕾,黄文芝
(武汉工程大学计算机科学与工程学院,湖北 武汉 430074)

摘　要:针对点对点网络中信任的模糊性和随机性难以刻画和计算的特点,首先运用域的概念设计一个信任模型,包括可信度的管理、传递和表示.在计算对等点的全局可信度时引入动态权重函数,再运用云理论将每个已存在的可信度映射为定量的可细微变化的不同云滴,并计算不同权值下其云的数字特征.在 Microsoft Visual C++和 Matlab 环境下,计算与标准概念云的相似度,相似度最大的云最大限度地保留了点对点网络中信任的随机度和模糊度,其所对应的权重最终确定了请求对等点的可信度.结果表明,运用域的概念和云理论的信任模型较好地表征和计算了点对点网络中的信任,具有较强的抗攻击能力.

关键词:点对点网络;云理论;域;信任模型;可信度
中图分类号:TP393　　**文献标识码**:A　　**doi**:10.3969/j.issn.1674-2869.2012.10.017

0　引　言

随着互联网的普及和宽带技术的发展,以点对点网络为核心的软件产品正在为越来越多的网民所接受和喜爱.点对点网络产品在短短几年时间,用户的注册量不断增长,已成为许多网民不能离弃的上网伙伴.一旦点对点网络应用发展到一个引人关注的程度,信任和安全问题就出现了.在用户间互相了解的小型应用中,信任和安全很少会成为问题.可是,有用的点对点网络应用很少会保持这么小的规模.人们围绕点对点网络的信任问题提出了许多有价值的信任模型.例如,EigenTrust[1]模型和基于 EigenTrust 改进的 SWRTrust[2]模型都是基于信任的全局信任模型,它们能够在一定程度上解决恶意节点的协同作弊问题,但它们只考虑了信任的随机性,都没有综合考虑信任的模糊性[3].

云模型是在传统模糊集理论和概率统计的基础上建立起来的一种定性定量不确定性转换模型,它主要反映客观世界中事物或人类知识中概念的两种不确定性:模糊性(边界的亦此亦彼性)和随机性(发生的概率),并把二者完全集成在一起,构成定性和定量相互间的映射[4].

首先提出一种基于域的信任模型,再运用云理论把定性的信任度映射为定量的表达,即映射为可细微变化的不同云滴,最后进行相关的仿真试验并给出分析结果.

1　基于域的信任模型

首先,在信任模型中引入域的概念.之所以引入域,是借鉴了人们在日常生活中的信任习惯:人们总是会相信他自己生活圈中的朋友,而对于圈外人士,人们就会比较小心谨慎些.下面介绍域的构架.

1.1　可信度的管理

评定官对等点 LP(Leader Peer)是在域中具有足够带宽、处理能力以及有较高的信任度的对等点,它来负责域中共享资源的目录管理.在 LP 上存放着两份列表,一份是它管辖范围内的对等点,另一份是其他 LP 的地址信息.很重要的一点,就是要对 LP 上的信息进行备份存储管理,以保证可信的管理.

1.2　可信度的传递

若 A 知道 B 的 IP 地址和端口号时,将要求它所属的 LP 返回 B 的可信度 t;若 A 知道 B'的 IP 地址和端口号时,则 A 所属的 LP 根据 B'的 IP 和端口号,向网络中其他 LP 转发对 B'的信任度 t'的查询,直到找到 B'所属的 LP,由它返回 B'的信任度 t[5].

1.3　可信度的表示

在此,用 t 表示可信度.与可信度相关的有几个参数:s 表示信任度(Success rate),f 表示忠诚度(Faithfulness).

信任的度量不仅要靠别人的推荐,也需要亲

收稿日期:2012-08-30
作者简介:张　蕾(1982-),女,河南信阳人,讲师,硕士.研究方向:可信度计算,密码算法等.

自和请求资源的结点交易后获得的直接信任值来共同决定.直接信任值指的是两个实体间根据过去相互间发生的直接交往行为而得出的信任等级关系.所谓某个实体的推荐值指的是其他实体通过观察其过去行为并根据其表现而得出的综合期望值[6].在进行信任决策时,当两个实体间过去没有直接的信任交往接触时,往往可借助对方的推荐值(也称间接信任)来抉择.

推荐这一决策是追加信息的场合.假定信息源的推荐者群为 x_k.他对实体 j 的推荐值 $r_{kj}\in[0,1]$ 是已知的,其中 0 表示不推荐,1 表示绝对可信.则推荐者对实体 j 的推荐值计算如下:

$$s_{ikj}=\sqrt{r_{kj}*t_{ik}} \tag{1}$$

其中,t_{ik} 表示实体 i 对推荐者 x_k 的信任度,$t_{ik}\in[0,1]$,0 表示不信任,1 表示绝对信任. 表示实体 i 根据推荐者 x_k 给的推荐值间接求出的对 j 的信任度.

这里所讨论的忠诚度是基于点对点网络中的一种不道德现象:有些用户怕影响硬盘寿命而"只下载不上传".这是一种自私自利的体现.对于上传文件越多的对等点,设置它的忠诚度越高[6].

$$f=\text{上传次数}/(\text{上传次数}+\text{下载次数}) \tag{2}$$

考虑到不同的参数对信任度的影响程度不同,需要对参数进行区分对待.本文按照影响程度不同给各个参数设定相应的权值 w_i,根据用户的要求不同灵活调整权值的分配.

$$x=w_1*s+w_2*f \tag{3}$$

式(3)中 $w_1+w_2=1$.

2 云理论

2.1 云理论介绍

设 U 是一个用精确数值表示的定量论域,$X\in U$,T 是 U 空间上的定性概念,若元素 $x(x\in X)$ 对 T 的隶属的确定度 $CT(x)\in[0,1]$ 是一有稳定倾向的随机数,则概念 T 从论域 U 到区间 $[0,1]$ 的映射在数域空间的分布,称为云(Cloud)[7].

云的数字特征反映了定性概念的定量特性,用期望 E_x(Expected value)、熵 E_n(Entropy)和超熵 H_e(Hyper entropy)三个数值来表征[8].云的数字特征 $C(E_x,E_n,H_e)$ 是描述云模型、产生虚拟云、实现云计算、完成云变换的数值基础[9].

期望 E_x:反映相应的模糊概念的信息中心值.

熵 E_n:反映相应的模糊概念的亦此亦彼的度量,也反映云滴的离散程度.

超熵 H_e:衡量偏离正态分布的程度,即云的分散性,反映了熵 E_n 的稳定性[10].

2.2 基于云理论的节点可信度量化模型

对点对点网络中任意一对等点 p_i,把迄今为止的对 p_i 的全部可信度记为 $X=\{x_i\mid x_i\in[0,1],i=1,2,\cdots,N\}$[11].样本集 X 的 E_x 为

$$E_x=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{4}$$

$$E_n=\frac{1}{N}\sqrt{\pi/2}\sum_{I=1}^{N}|x_i-E_x| \tag{5}$$

$$H_e=\sqrt{\frac{1}{N-1}\sum_{I=1}^{N}(x_i-E_x)^2-E_n^2} \tag{6}$$

因为用户对可信度的要求会有不同,而不同要求下各参数对可信度的影响程度也不一样,所以本文考虑了动态权重,根据用户需求动态调整权重的分布.实验中考虑到的三种权重如表 1 所示.

表 1 不同的权重取值

Table 1 Different values of weight

权重	信任度	忠诚度
权重 1	0.6	0.4
权重 2	0.7	0.3
权重 3	0.9	0.1

2.3 基于云理论的对等点可信度量化算法

基于云理论的对等点可信度量化算法描述如下:

Step 1 初始化.输入 p_i 整个生存期所有的可信度相关参数[11].

Step 2 根据不同的权重,分别计算 x_i.

Step 3 根据公式(4)、(5)、(6)计算 E_x,E_n,H_e.

Step 4 绘制出云,找出随机度和模糊度最小的参数所对应的权重.

3 仿真实验及分析

本文所用实验平台为 VC 和 MATLAB 7.0.

信任度是用户最在乎的因素,因此本文重点对信任度进行研究.被评价对等点的信任度产生办法为:分别以 0.3,0.4,0.5,0.6,0.7,0.75,0.8,0.9 为基数,叠加分布为 $x\sim N(0,0.02^2)$ 的高斯噪声序列,产生 1 000 个数据,作为其迄今为止生命期内得到的信任度.各基数下的数据分布如表 2 所列.忠诚度采用 0~1 的随机数产生器产生[12].

表 2 各基数下数据分布表

Table 2 Data distribution list in different cardinal number

	数据基数							
	0.3	0.4	0.5	0.6	0.7	0.75	0.8	0.9
数据个数	5	5	20	70	800	70	20	10

根据所获得的信任云数字特征生成的正向信任云分别如图 1 和图 2 所示,它们的云滴数分别为 500 和 1 000. 可以看出,两个正向信任云与样本集 X 的信任云具有相似的整体分布特征. 且随着云滴数的增加,信任云的整体特征更为明显. 这成为采用对等点正向信任云指导其信任量化的依据[13].

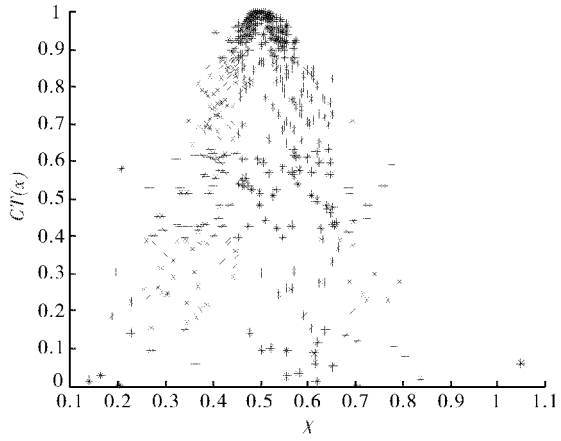

图 1　权重 1 下 500 个对等点信任云

Fig. 1　Trust cloud of 500 peers in weight 1

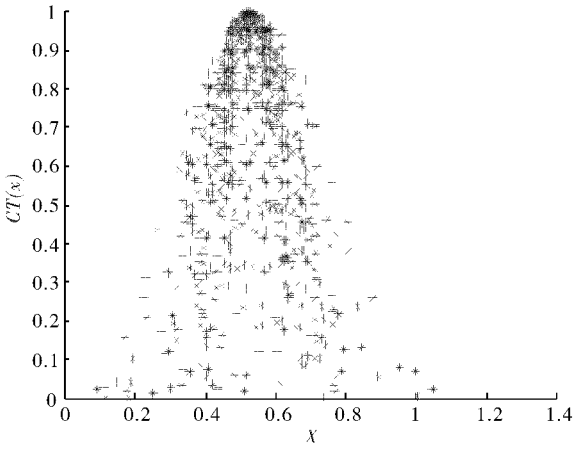

图 2　权重 1 下 1 000 个对等点

Fig. 2　Trust cloud of 1 000 peers in weight 1

图 2、图 3、图 4 分别为表 1 三种不同权重下得到的结果可以看出,图 2、图 3、图 4 中的云的期望相差不大,但是图 3 中云的熵和超熵都最小,图 2 中云的熵和超熵其次,图 4 中云的熵和超熵最大,因此图 4 建模出来的信任度的随机度和模糊度最大. 由此说明权重 2 的情况下建模效果最好,被选择作为可信度权重,权重 1 居其次,权重 3 最差. 综上可知,在不同的情况下给各参数加以不同的权重得出的结果是不一样的,为了满足用户不同的需求,在云模型原有基础上加入动态分配权重功能,为用户需求找到合适的权重分配,才能建模出更贴近实际的信任情境.

本模型有很强的抗攻击性. 这是因为恶意对等点很难改变按照被评价对等点整个生命期内的可信度样本集 X 获得的其云数字特征值. 依照此数字特征值的可信度计算,偏离云期望的可信度将获得趋低倾向的确定度值,进而获得很小的权值. 因而,即使攻击数量很多,模型也表现出极强的抗攻击性. 因此,本文的可信度计算模型在抗攻击性方面表现出明显的优越性.

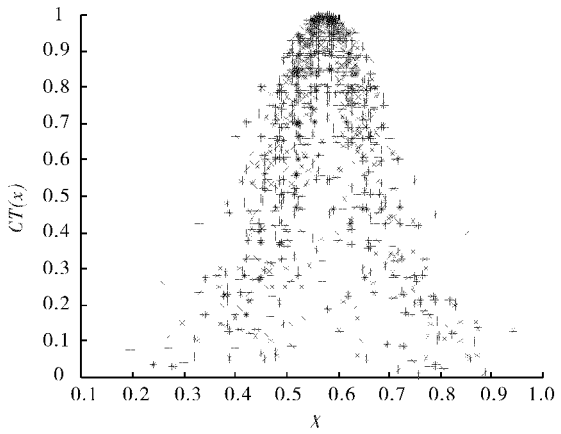

图 3　权重 2 下 1 000 个对等点

Fig. 3　Trust cloud of 1 000 peers in weight 2

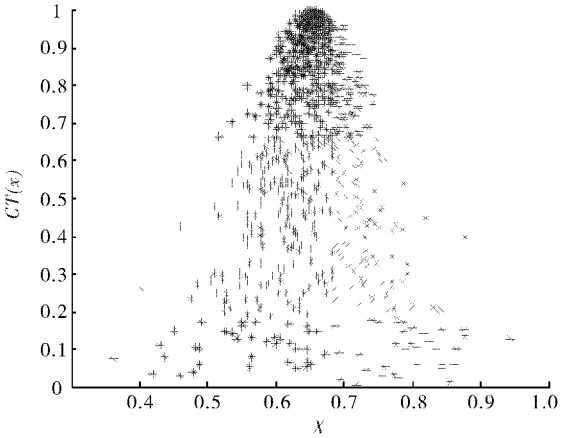

图 4　权重 3 下 1 000 个对等点信任云

Fig. 4　Trust cloud of 1 000 peers in weight 3

4　结　语

点对点网络技术已经广泛应用于网络交易中,分布式网络使用户处于孤立地位. 以上提出的基于域的信任模型,从而使得用户在网络中建立了自己的“朋友域”,方便了用户之间的直接交易. 用户需要其他“非朋友域”用户的资源,需要对其他用户有个信任评价. 在本文中,为了评价不确定的信任度,采用了云理论. 它能够在广度和深度上科学地描述对等点在其生命期内的信任情况,实现信任度这定性概念的合理量化,揭示了对等点信任聚合过程中的模糊性和随机性规律,且具有较强的抗攻击能力. 因此,该研究是符合用户需要及点对点网络发展需要的. 如何更合理及更准确

地采样影响系统的性能参数,以使得计算结果更科学可信,是下一步研究的方向.

参考文献:

[1] Kamver S D, Schlosser M T, Garcia-Molina H. The Eigentrust Algorithm for Reputation Management in P2P Networks[C]//Proc. of the 12th Int'l World Wide Web Conference. Hungary: Budapest, ACM Press, 2003: 640-651.

[2] 李景涛, 荆一楠, 肖晓春, 等. 基于相似度加权推荐的P2P环境下的信任模型[J]. 软件学报, 2007, 18(1): 157-167.

[3] 李小勇, 桂小林. 可信网络中基于多维决策属性的信任量化模型[J]. 计算机学报, 2009, 32(3): 405-416.

[4] 宋远骏, 杨孝宗, 李德毅, 等. 考虑环境因素的计算机可靠性云模型评价[J]. 计算机研究与发展, 2001, 38(5): 631-636.

[5] 司聿宣,苏远兴,杨正芳. 分布式环境实时语音通讯系统的设计与实现[J]. 武汉工程大学学报, 2012, 34(5): 60-63.

[6] 王守信, 张莉, 李鹤松. 一种基于云模型的主观信任评价方法[J]. 软件学报, 2010, 21(6): 1341-1352.

[7] Wu D, Mendel J M. A comparative study of ranking methods, similarity measures and uncertainty measures for interval type-2 fuzzy sets[J]. Information Sciences, 2009, 179(8): 1169-1192.

[8] Li Deyi, Liu Chang Yu, Gan Wenyan. A new cognitive model: Cloud model [J]. International Journal of Intelligent Systems, 2009, 24(4): 357-375.

[9] Li Tao. An immunity based network security risk estimation [J]. Science in China Series F: Information Sciences, 2005, 48(5): 557-578.

[10] Wang Shouxin, Zhang Li, Li Hesong. Evaluation approach of subjective trust based on cloud model [J]. Journal of Software, 2010, 21(6): 1341-1352.

[11] Li Deyi, Du Yi. Artificial intelligence with uncertainty [M]. Beijing: National Defense Industry Press, 2005: 178-186.

[12] 雷建云,余涵,蒋天发,等. 自动信任协商中的敏感信息保护方案[J]. 武汉理工大学学报, 2012,34(3):137-140.

[13] 田春岐, 邹仕洪, 王文东, 等. 一种基于推荐证据的有效抗攻击P2P网络信任模型[J]. 计算机学报, 2008, 31(2): 270-281.

Trust domain model in peer-to-peer network by using cloud theory

ZHANG Lei*, *HUANG Wen-zhi

(School of Computer Science and Engineering, Wuhan Institute of Technology, Wuhan 430074, China)

Abstract: As the fuzziness and uncertainty of trust could not be described and calculated exactly in peer-to-peer network, a trust model using domain concept was designed firstly, including management, transmission and expression of trust degree. In the calculation of the peer global trust value, dynamic weight function was introduced. Then, each qualitative existed trust degree was mapped to quantitative and variable cloud droplet by using cloud theory, and numerical characteristics of every cloud were calculated with different weight. In Matlab and Microsoft Visual C++, similarity with standard cloud was calculated, the cloud which was the most similar to the standard kept furthest fuzziness and uncertainty of trust in peer-to-peer network, and ultimately the request peer trust degree was determined. The result shows that the trust model based on domain concept and cloud theory describes and calculates the trust in peer-to-peer network, and it also has strong ability against the attack.

Key words: peer-to-peer network; cloud theory; domain; trust model; trust degree

本文编辑:陈小平